ABC Working Group

General Counsel
84-263

January 16, 1984

M E M O R A N D U M

TO: Working Group on Intelligence Requirements and Criminal Code Reform

FROM: Axel Kleiboemer

---

Attached is Mr. Martin's report which will be on the agenda for our meeting on January 23rd. In addition, I anticipate that Mr. Clarke will have the re-draft of his position paper available for discussion.

AK/sd
Attachment

LAW OFFICES

JENNER & BLOCK

A PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS

21 DUPONT CIRCLE, N.W.

WASHINGTON, D.C. 20036

(202) 466-5470

CHICAGO OFFICE

ONE IBM PLAZA

CHICAGO, ILLINOIS 60611

(312) 222-9350

THOMAS S. MARTIN

January 11, 1984

Axel Kleiboemer, Esq.
Santarelli & Bond
Suite 700
2033 M Street, N.W.
Washington, D.C. 20036

Dear Axel:

Enclosed is the promised draft of the proposed legislation and an advisory note for discussion at our meeting on January 23, 1984. I assume that your office will circulate these materials to the other members of the Task Force.

Sincerely yours,

Thomas S. Martin

Enclosures

DRAFT CRIMINAL LEGISLATION
PROHIBITING DISCLOSURE OF
RESTRICTED DEFENSE INFORMATION

AN ACT to amend the National Security Act of 1947 to prohibit the unauthorized disclosure of restricted defense information

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Defense Information Protection Act of 1983."

Sec. 2.(a) The National Security Act of 1947 is amended by adding at the end thereof the following new title:

"TITLE VII -- PROTECTION OF RESTRICTED DEFENSE INFORMATION

PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION

Sec. 701. (a) Whoever, having or having had authorized access to restricted defense information, intentionally discloses any such information to any individual not authorized to receive classified information, knowing that the information disclosed is restricted defense information, shall be fined not more than $50,000 or imprisoned not more than twenty-five years, or both.

(b) Whoever, as a result of having authorized access to classified information, obtains restricted defense information and intentionally discloses such information to any individual not authorized to receive classified information, knowing that the information disclosed is restricted

defense information, shall be fined not more than $25,000 or imprisoned not more than fifteen years, or both.

(c) Whoever, not as the result of having authorized access to classified information, obtains restricted defense information and intentionally discloses such information to any individual not authorized to receive classified information, knowing that the information disclosed is restricted defense information, shall be fined not more than $15,000 or imprisoned not more than ten years, or both.

DEFENSES AND EXCEPTIONS

Sec. 702. (a) It is a defense to a prosecution under section 701 that before the commission of the offense with which the defendant is charged, the United States had previously publicly acknowledged the secrecy of the restricted defense information.

(b) It is a defense to a prosecution under section 701(a) that the disclosure was authorized by the United States Government pursuant to regulations and procedures promulgated to provide official sanction for disclosures of restricted defense information.

(c) No person other than a person committing an offense under section 701 shall be subject to prosecution under such section by virtue of section 2 or 4 of title 18, United States Code, or shall be subject to prosecution for conspiracy to commit an offense under such section.

(d) It shall not be an offense under section 701 to transmit restricted defense information directly to the Select Committee on Intelligence of the Senate or the Permanent Select Committee on Intelligence of the House of Representatives.

REPORT

Sec. 703. (a) The President, after receiving information from the Director of Central Intelligence and the Attorney General, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives an annual report on measures to protect restricted defense information and on the operation and effectiveness of this Title, including suggested amendments to this Title.

(b) The report described in subsection (a) shall be exempt from any requirement for publication or disclosure. The first such report shall be submitted no later than February 1, 1985.

EXTRATERRITORIAL JURISDICTION

Sec. 704. There is jurisdiction over an offense under section 701 committed outside the United States if the individual committing the offense is a citizen of the United States or an alien lawfully admitted to the United States for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act).

PROVIDING INFORMATION TO CONGRESS

Sec. 705. Nothing in this title may be construed as authority to withhold information from the Congress or from a committee of either House of Congress.

DEFINITIONS

Sec. 706. For the purpose of this title:

(a) The term "restricted defense information" means information that is classified as Top Secret and

(1) is Restricted Data as defined in section 2014(y) of title 42, United States Code; or

(2) concerns the technical design of advanced weapons systems; or

(3) concerns sources and methods of obtaining communications intelligence.

(b) The term "classified information" means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

(c) The term "authorized," when used with respect to access to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or

agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.

(d) The term "disclose" means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

(e) The term "United States," when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands."

Sec. 2.(b) The table of contents at the beginning of such Act is amended by adding at the end thereof the following:

"TITLE VII -- PROTECTION OF RESTRICTED DEFENSE INFORMATION

Sec. 701. Protection of certain national security information.

Sec. 702. Defenses and exceptions.

Sec. 703. Report.

Sec. 704. Extraterritorial jurisdiction.

Sec. 705. Providing information to Congress.

Sec. 706. Definitions."

DRAFT/TSM
January 11, 1984

## Advisory Note

It is widely recognized that the criminal espionage laws do not provide an adequate response to the problems associated with the leak of national security information. Those laws were drafted for the purpose of deterring classic espionage by individuals whose intention is to pass on classified information to foreign countries. In addition, those laws were not intended to address the question of publication of national security information by members of the press. See, "Can Democracy Keep Secrets?" Guenther Lewy, Fall 1983 Policy Review No. 26 at 17-29; Edgar and Schmidt, "The Espionage Statutes and Publication of Defense Information," 73 Col. L. Rev. 991, 998 (1973).

In fact, the publication of information by individuals whose asserted intentions are to advance public debate rather than aid foreign countries has become a problem of increasing significance. The Government response to the serious disclosures which have occurred has included efforts to obtain prior restraints upon publication and the development of a line of cases establishing a civil penalty involving forfeiture of funds earned in violation of secrecy agreements. See United States v. Snepp, 444 U.S.

507 (1980); United States v. The New York Times, 403 U.S. 507 (1980); United States v. The Progressive, 467 F. Supp. 990 (W.D. Wis. 1979).

Unfortunately, neither remedy provides sufficient protection for national security values. In part, because of the constitutional presumption against prior restraints, the pursuit of that remedy has not only been a practical failure but has resulted in counter-productive confirmation of the validity of disclosed material. Similarly, the Snepp remedy is limited in deterrent value because its impact is solely monetary and its scope extends only to government employees who may have signed a secrecy agreement. See Martin, "National Security and the First Amendment," ABA Journal, June 1982, pp. 680-685. Congress has acted to address some portion of the gap in criminal law enforcement by enactment of the Intelligence Identities Protection Act. On the other hand, the existence of this legislation creates an anomaly because other categories of disclosure of equal or greater national security importance are totally unaddressed.

The proposed legislation is designed to provide enhanced protection for the national security of the United States against non-espionage disclosures of national security information. It rests upon three propositions: (1) that there exists a category of information so important

to the maintenance of the national defense that it should not be disclosed under any circumstances by any party; (2) that this category of information does not include all classified information but rather should be defined as narrowly as possible and (3) that criminal law penalties against such disclosure would have a practical deterrent effect. The format of the proposed legislation generally follows that of the Intelligence Identities Protection Act. It is designed to build upon the positive Congressional experience in enacting that legislation.

The first part of the legislation establishes a category of national security information termed "restricted defense information," the disclosure of which would generate liability under the statute. The term restricted defense information is defined in Section 706. Subject matters included within the term are nuclear weapons technology, technical information relating to the design of advanced weapons systems and information the disclosure of which will reveal sources and methods of obtaining communications intelligence. Discussions with representatives of the national security agencies have resulted in a consensus that the information described is in fact the most sensitive category of national defense information that exists. Notably, the category does not include historical information or information relating to policy of the kind, for

example, that was disclosed in the Pentagon Papers. It is the Committee's view that the disclosure of such information can best be dealt with through existing procedures relating to the care of classified information. In addition, it should be noted that to generate liability under the proposed statute, information must not only fall within the generic category described, but must in fact be properly classified as top secret under the current classification system.

The proposed statute prohibits any knowing disclosure of the specified information without regard to the purposes of the disclosing party. It is the conclusion of the Task Force that placing within the statute a requirement of intent to injure the United States or to provide information to foreign governments would result in legislation which is no more useful than the current espionage statutes.

In addition, the statute is designed to create criminal liability with respect to all parties in the chain of disclosure. Government officials are vulnerable to prosecution whether they are at the highest level of government or the lowest. This is a deliberate decision to avoid the problems of selective prosecution and the fear that government officials may be able to use information to their political advantage while the hands of the responsive press are tied. High government officials wishing to

disclose restricted defense information pursuant to their official responsibilities, however, can obtain authorization to do so, but only pursuant to procedures and regulations promulgated for that purpose. See Section 702(b).

Similarly, the law explicitly applies to all disclosures including those made through publication by members of the press. See Section 706(d). The application to all disclosures including those by the press results from a judgment that the harm to the country results from disclosure irrespective of the party who makes the disclosure. The constitutionality of the application of criminal law in this context to members of the press has not been definitively decided; however, the decisions that are available indicate that a carefully and narrowly drawn statute would pass constitutional muster. The press has no greater constitutional interest in free expression or in access to information than does any individual. Nixon v. Warner Communications, Inc., 435 U.S. 589, 609-10 (1978); Saxbe v. Washington Post Co., 417 U.S. 843, 850 (1974); see First National Bank v. Bellotti, 435 U.S. 765, 797-802 (1978) (Burger, C.J., concurring).

The language of the proposed statute does not differentiate between disclosures depending upon their source. Again, this reflects a deliberate judgment that this category of information should not be published

irrespective of whether the ultimate source is a government document, a high public official or an accidental disclosure. The penalties imposed by the statute do vary, however, depending upon the level of trust reposed by the government in an individual as a result of his access to either restricted defense information or other classified information. See Section 701(a)(b) and (c). However, no prosecution is authorized when the information has previously been publicly acknowledged by the United States since the secrecy of the information would have been compromised in such circumstances. See Section 702(a).

A final issue is whether the statute should be enforced by the Attorney General. Prosecutions of the kind contemplated may often be unpopular, and experience under the espionage laws indicates to some that the Attorney General may decline prosecution for political reasons. Similarly, this legislation might theoretically be enforced only against members of the press and ex-government officials, and not be enforced against high government officials who, without proper authorization, decide to use the sensitive information for what they view as a positive public purpose. The Committee has given consideration to the appointment of a Special Prosecutor for the purpose of enforcing this statute. On balance, the draft legislation proposes that initial enforcement be placed within the responsibilities

of the Attorney General. Section 703 of the legislation also requires, however, a report of the Congress within a 12 month period concerning actual experience in enforcement of the law. Should the experience prove the fears which have been suggested to be well taken, we would anticipate Congressional action to establish a Special Prosecutor to enforce the legislation.